Risk Assessment Guidelines for the Investment Analysis Process

Update of July 1999

Prepared for
Investment Analysis and Operations Research, ASD-400
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591

Prepared by
Operations Assessment Division, DTS-59
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142

Report No. WP-59-FA7N1-97-2

Table of Contents

Intentionally Left Blank

Preface

This document presents guidelines for conducting life cycle risk assessments as part of the Federal Aviation Administration's (FAA's) Investment Analysis Process (IAP) as proscribed in the *Acquisition Management System, Investment Analysis Process: Guidelines*, July 1998. The guidelines are intended to be used by Investment Analysis Teams (IATs) in the analysis of candidate alternatives/solutions.

The guidelines were developed by James L. Poage of the Operations Assessment Division (DTS-59), John A. Volpe National Transportation Systems Center, Research and Special Projects Administration, and by Paul D. Abramson and Edmund J. Koenke of System Resources Corporation. The work was performed for Investment Analysis and Operations Research, ASD-400. Daniel Citrenbaum of ASD-400 made major contributions to the risk assessment guidelines presented in this document. The guidelines were adapted from similar guidelines developed for supporting management of the FAA Research, Engineering and Development (R,E&D) investment portfolio.

Risk assessment can be viewed as a dynamic enterprise. As the National Airspace System (NAS) operations and environment change, we would expect that new issues and risks affecting investment analysis would surface. Since the first publication of these Guidelines in July 1997, information security, human factors, and safety issues have gained visibility and prominence as additional risk to be considered. Accordingly, in July 1999, Art Politano (ASD-400) and Don Weitzman, Systems Engineering Technical Assistance (SETA) updated the set of risk facets to include their assessment.

Intentionally Left Blank

RISK ASSESSMENT GUIDELINES
FOR INVESTMENT ANALYSIS PROCESS

1.0 INTRODUCTION

The *Acquisition Management System, Investment Analysis Process: Guidelines*, July 1998, describes the Investment Analysis Process (IAP) to be used during the investment analysis phase of a Federal Aviation Administration (FAA) acquisition program activity. The IAP proscribes an Investment Analysis Team (IAT) to analyze candidate alternatives/solutions. An evaluation matrix is to be constructed containing a value or ranking for each alternative's evaluation factors. Evaluation factors include[1]:

- Life cycle costs
- Benefits
- Schedule
- Performance
- **Risk**

This document describes a process to assess the **Risk** evaluation factor for each alternative. The word "alternative" is used in the following text to refer to the candidate alternative/solution for which the risk is being assessed. The risk assessment process is applied to each alternative.

Risk[2] is defined as the probability of an undesirable event occurring combined with the consequence of the occurrence. In the context of this document, risk is the probability that an alternative will fail to deliver the benefits projected for that alternative, either in whole or in part, and the consequences of this failure. The risk can derive from uncertainties in the alternative's concept or problems encountered during design, development, implementation, or operation.

Often the sensitivity analysis of the benefit and cost estimates in a benefit/cost analysis is considered to be a risk analysis. For this document, life cycle risk assessment is the assessment of the probability that an alternative will fail to deliver the projected benefits and the consequences of such a failure. Any sensitivity analysis of benefit and cost estimates is to be completed as part of the benefit/cost study. However, this risk assessment does address the perceived accuracy of the benefit and cost estimates, whether the link of the alternative to projected benefits is tenuous, and whether the project is defined enough to estimate the benefits and costs. In addition, the risk assessment addresses risks in achieving technical performance, operational performance, supportability, and other factors.

The risk assessment results from the process described in this paper can not only be used as part of decision-making on an alternative, but also to manage risk throughout the acquisition cycle.

---

[1] *Acquisition Management System, Investment Analysis Process: Guidelines*, July 1, 1998, p. 10.

[2] The risk assessment process described in this paper draws heavily upon and adapts risk assessment concepts described in *Acquisition and Program Risk Management Guide*, Revision 1, FAA-P-1810, September 29, 1995.

Intentionally Left Blank

2.0 DEPENDENCIES WITH OTHER PROGRAMS

In assessing the life cycle risk of an alternative, any linkages of the alternative with other programs must be considered. These linkages should consider other projects necessary for the subject alternative to be completed or other projects that will provide synergy with the subject alternative and result in benefits listed in the benefit assessment. Linkages must be documented in the risk assessment submission as a statement of alternative dependencies:

Describe the relationship to other projects. Examples of questions to address are:

- ⇒ Is the outcome of this alternative dependent on input from another project;
- ⇒ Is this alternative dependent on the performance of another project; or
- ⇒ Is this alternative dependent upon the activities of another agency, such as NASA or DoD.

Describe and provide evidence that:

- ⇒ The plans and budgets among related projects are coordinated, or
- ⇒ The alternative has no relationship to other projects.

Intentionally Left Blank

3.0 LIFE CYCLE RISK ASSESSMENT

These guidelines consider the risks associated with the design, development, implementation, and operation phases of an alternative. Thus, the entire life cycle of the alternative is included.

3.1 Risk Facets

The life cycle risks are broken down into thirteen components, or facets, of risk, which are used to assess the overall risk. These risk facets have been selected to reflect the risks associated with alternative completion, operation, and achieving the projected benefits and to facilitate the risk identification and quantification processes. The thirteen risk facets are defined as follows:

- **$Risk_{Technical}$** is the risk associated with (1) developing a new or extending an existing technology to provide a greater level of performance than previously demonstrated, or (2) achieving an existing level of performance subject to new constraints. It also refers to how well the system operates to design or safety specifications.

- **$Risk_{Operability}$** is the risk associated with how well the system to be produced will operate within the National Airspace System (NAS) and interact with other systems. It addresses NAS or other system interfaces, the degree to which they are known and complete, and the degree to which the operational concept has been demonstrated and evolved to the point of a design baseline.

- **$Risk_{Producibility}$** is the risk associated with the capabilities to manufacture and produce the desired system.

- **$Risk_{Supportability}$** is the risk associated with fielding and maintaining the resulting systems.

- **$Risk_{Benefit\ Estimate}$** considers the difficulty in estimating the benefits. This risk facet addresses the accuracy of the benefit estimate, including such issues as inadequate methods to estimate the benefits, lack of data to estimate the benefits, whether the link of the alternative to projected benefits is tenuous, and whether the alternative is defined enough to estimate the benefits.

- **$Risk_{Cost\ Estimate}$** considers the difficulty in estimating the cost. This risk facet addresses the accuracy of the cost estimate, including such issues as inadequate methods to estimate the cost, lack of data to estimate the cost, and whether the alternative is defined enough to estimate the cost.

- **$Risk_{Schedule}$** considers the likelihood that the alternative will be completed within the specified schedule.

- **$Risk_{Management}$** refers to complexity of the alternative to manage (e.g., number of sub-tasks and/or number of performing organizations) and considers the risks of obtaining and using applicable resources and activities which may be outside of the alternative's control but can affect the alternative's outcome.

- **$Risk_{Funding}$** addresses the availability of funds when they are needed and a confidence in management and Congress that those funds will continue to be provided.

- **$Risk_{Stakeholder}$** is the risk associated with various stakeholders supporting the development and operation of the alternative, such as internal FAA organizational users, Congress, airline and general aviation users, and potential equipment and aircraft manufacturers.

- **$Risk_{Information\ Security}$** addresses a system's vulnerability to external threats and the risks likely to occur in employing countermeasures.

- **$Risk_{Human\ Factors}$** focuses on the effectiveness of the joint human-system interface and risks associated with making the system usable in an operating environment.

- **$Risk_{Safety}$** considers the likelihood of system related hazards and the risks associated with preserving operational safety.

3.2 Interaction of Risk Facets with Final Benefits and Costs

All thirteen risk facets ultimately affect the successful completion and implementation of any alternative and, hence, affect the final benefits and cost. Thus, the risk facets **$Risk_{Benefit\ Estimate}$** and **$Risk_{Cost\ Estimate}$** may appear to be influenced by the other eleven risk facets. This potential difficulty is handled by careful definition of what is included in **$Risk_{Benefit\ Estimate}$** and **$Risk_{Cost\ Estimate}$.**

There are two distinct types of risk associated with the final benefits and costs. The first type is the risk that the project will not be successfully implemented within the estimated costs and that it will not achieve the estimated benefits, assuming that the benefits and costs are accurately estimated. The second type of risk has to do with the inherent accuracy of the benefit and cost estimates, assuming that the alternative is successfully implemented.

In the former case, implementing the project within the estimated cost and achieving the estimated benefits are functions of the other eleven risk facets, that is technical, operability, producibility, supportability, schedule, management, funding, and stakeholder. For example, a technical problem in achieving adequate capacity or a producibility problem involving unavailable equipment can adversely affect both the cost of the project and the full realization of the potential benefits.

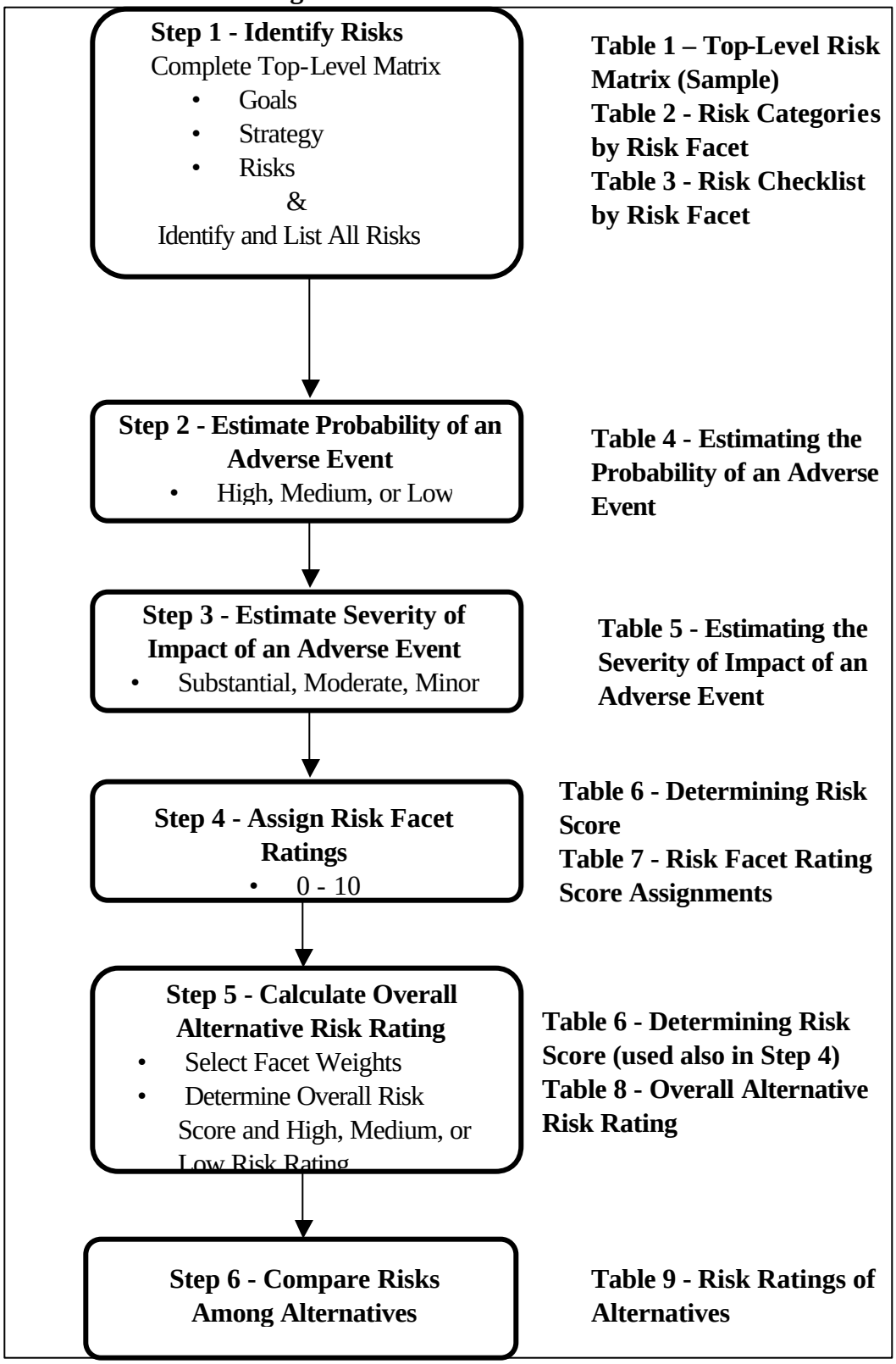
In contrast in the latter case, $\mathbf{Risk_{Benefit\ Estimate}}$ and $\mathbf{Risk_{Cost\ Estimate}}$ deal with the accuracy of the benefit and cost estimates, such as inadequate methods and/or data to estimate benefits and cost. If the benefits and costs are estimated inaccurately, the project could be conducted and implemented perfectly and still not meet the benefit and cost estimates due to the errors in the estimates of these values. $\mathbf{Risk_{Benefit\ Estimate}}$ and $\mathbf{Risk_{Cost\ Estimate}}$ address the difficulty in estimating the benefits and costs, whether the link of the alternative to projected benefits is tenuous, and whether the alternative is defined sufficiently to confidently estimate the benefits and costs.

Thus, all thirteen risk facets combine into an overall risk assessment that includes (1) whether the alternative will be successfully implemented within the estimated cost estimate and achieve the projected benefits and (2) the difficulty in estimating the benefits and cost of the alternative. Only this overall risk assessment addresses the ultimate successful achievement of the desired benefits of the alternative within the planned cost.

3.3 Introduction to Risk Assessment Process

The steps of the risk assessment process in the IAP are shown in Figure 1, Risk Assessment Process. The figure outlines the steps to identify and quantify risks and relates those steps to various tables in this document.

Figure 1. Risk Assessment Process



4.0 CONDUCTING THE RISK ASSESSMENT PROCESS

The six steps for risk assessment, listed in Figure 1, are presented below along with tables to assist the process.

4.1 Step 1 - Identify Risks

Risks cannot be assessed or managed until they are identified and described in an understandable way. Risk identification is an organized and thorough approach to seek out risks associated with an alternative. It is not a process of trying to invent highly improbable scenarios of unlikely events in an effort to cover every conceivable future possibility.

A **Top-Level Risk Matrix** (Table 1 shows a sample) is employed for each alternative to assure a structured and consistent risk identification process for the thirteen risk facets and to document the results. Completing Table 1 for each alternative to identify that alternative's risks involves three steps:

- Define Goals Relating to Risk Facets - Goals (for the alternative being assessed) which address potential risks in each risk facet are defined in the Top-Level Risk Matrix, Table 1. By defining goals as they relate to mitigating the potential risks in each risk facet, the specific risks that will be important to the alternative can be more easily identified. This information will also aid the process in Steps 2 and 3 to quantify the risks.

  Requirements specified in a Requirements Document should be considered in defining goals. If the requirements are not explicit enough to yield goals related to the risk facets, this process identifies that fact and goals should be developed. A goal block that cannot be completed satisfactorily is an alert, and some action should be precipitated to fill the void.

- Define Plans Relating to Risk Facets - Plan(s) for achieving the goals related to each risk facet, and hence mitigating risks, are also listed in the Top-Level Risk Matrix. The Top-Level Risk Matrix serves as a forcing function to insure there are plans to address all goals.

- Identify Risks - Risk identification involves identifying the risks pertaining to each risk facet for successfully completing and implementing the alternative. The goals and plans related to each risk facet will aid in identifying the risks that are important.

It is not necessary, nor in many cases appropriate, to complete the above three steps sequentially. Iterating among the steps may be helpful. As more risks are listed, the goals and plans may be revised and visa versa. The risks listed under each risk facet in Table 1 will provide the basis for the risk quantification in the next section. The statement of program goals relating to the risk categories and the plans for mitigating the risks will help quantify the risks.

Table 1, Top-Level Risk Matrix (Sample), is presented with sample entries in each box to clarify how the table is used. The sample entries are constructed for a possible alternative related to satellite surveillance.

Table 1. Top-Level Risk Matrix (Sample)

RISK FACET	RISK IDENTIFICATION	
Technical	**Goals:**	To transition from ground-based radar surveillance to a joint satellite and ground-based surveillance system.
	Plans:	Formulate requirements for, develop, and implement new technology to provide joint satellite and ground-based surveillance.
	Risks:	• Undue reliance on currently unavailable or unproved technology. • No or minimal prototype testing. • Inaccurate/simplistic modeling.
Operability	**Goals:**	To provide users and the FAA with operational benefits, such as the implementation of free flight.
	Plans:	Determine the surveillance requirements of free flight and other advanced automation programs in order to provide a design that fully satisfies these requirements.
	Risks:	• Incompatibilities with future NAS systems. • Incompatible or inconsistent operations with existing systems or regulations. • Uncertain operational requirements of the other programs
Producibility	**Goals:**	To develop and manufacture ground-based and aircraft-based system components to meet requirements and be within the cost estimates.
	Plans:	Use non-developmental items (NDI) and commercial off-the-shelf (COTS) items, and integrated NDI/COTS to the extent possible.
	Risks:	• Custom design & manufacture required.
Supportability	**Goals:**	To provide support for both existing and new surveillance systems during transition to the new system.
	Plans:	Coordinate closely with Airway Facilities (AF), including the field, and establish the Project Office within the appropriate Integrated Product Team.
	Risks:	• Satellite support not under FAA control. • Unclear Logistics Center responsibilities. • Existing system may not be maintainable over the implementation period required for new system.
Cost Estimate	**Goals:**	To provide users and FAA with benefits, such as free flight, within estimated program cost.
	Plans:	Implement cost control tools that will be used by the program office
	Risks:	• Speculative life-cycle costs. • User avionics costs difficult to estimate.

Table 1. Top-Level Risk Matrix (Sample), continued

RISK FACET	RISK IDENTIFICATION	
Benefit Estimate	**Goals:**	To provide users and FAA with benefits, such as free flight*, within estimated program cost.
	Plans:	Implement benefit identification, estimation, and tracking tools that will be used by the program office
	Risks:	• Difficult to identify benefits. • Difficult to estimate benefits.
Schedule	**Goals:**	To fully implement the new system by the year 20XX according to the schedule for the acquisition.
	Plans:	Initiate the acquisition program at the earliest possible time. Implement and maintain a program office with separate staff and budget and with the authority and responsibility for implementing new system.
	Risks:	• Insufficient schedule margin. • Schedule sensitive to technical complexity. • Uncertainties in contracting process. • Excessive task concurrency.
Management	**Goals:**	To provide the implementation planning, resources, and controls needed to accomplish the development and implementation while meeting the requirements, cost, and schedule estimates identified in the program plan.
	Plans:	Implement and maintain a program office with separate staff and budget and with the authority and responsibility for implementing new system.
	Risks:	• Inadequate program office staffing. • Inadequate resource allocation. • Inadequate authority. • Undefined integration responsibilities. • Unplanned slips in other programs. • Excessive span of control. • Uncontrolled requirements changes. • Requirements freeze not enforced.
Funding	**Goals:**	To obtain the required development and implementation funding identified in the program plan in a timely manner.
	Plans:	Obtain top-management support; reprogram available funding to get an early start on the acquisition alternative.
	Risks:	• Unfavorable agency priorities. • Inadequate funding.

Table 1. Top-Level Risk Matrix (Sample), continued

RISK FACET	RISK IDENTIFICATION	
Safety	**Goals:**	To minimize the Program's impact on the safety of the NAS.
	Plans:	Identify safety level objectives/ requirements/hazards and the criteria for acceptable risk for all ATM programs.
	Risks:	• Safety level objectives/requirements/hazards ambiguous, not fully characterized • Interdependent relationships contributing to system failure not fully considered • Acceptability criteria not fully known or understood for future NAS environments (e.g., free flight) • Mitigation strategies not palatable
Information Security	**Goals:**	To provide an information security infrastructure to protect NAS programs.
	Plans:	Formulate plans for the design, procurement, configuration, and maintenance of the information security infrastructure.
	Risks:	• Severity of system vulnerability ambiguously understood • Difficulty of threats to system not clearly understood. • Countermeasures have uncertain operational effectiveness
Human Factors	**Goals:**	To ensure an effective joint human-system interface for all NAS system development.
	Plans:	Determine the requirements for an effective joint human-system interface in order to provide a system design that is usable, useful, and acceptable to the user community.
	Risks:	• Requirement not fully or adequately defined • Fails to provide the necessary functionality • Is not acceptable to the user community.
Stakeholder	**Goals:**	To meet the user demands for more flexibility in flight paths.
	Plans:	Involve the user/international community in the system design and evaluation process.
	Risks:	• Resistance to avionics equipage requirements. • Diverse user community. • Conflicting user demands. • Conflicting user opinions.

As an aid in completing the risk lists in the Top-Level Risk Matrix, Table 1, a risk checklist should be used, such as that contained in Table 2, Risk Categories by Risk Facet, and Table 3, Risk Checklist by Risk Facet. Table 2 shows sample categories of risk elements, and Table 3 provides a comprehensive sample list of potential risks under each category. These tables can be used as a starting point for listing risks for any alternative, and other risks that may be pertinent should be added. Table 3 was made comprehensive to address all program stages at which a risk assessment might be done, and, hence, the table may contain risk elements not appropriate to the R,E&D phase or to a particular alternative being assessed.

The relevant items in the checklist should be evaluated to determine whether they apply to the particular alternative. Other potential risks not listed in the sample risk checklist in Table 3 should be added to the risk checklist for the particular alternative. The alternative's risk checklist should contain all possible risks that might be related to the alternative. After listing all possible risks, those which are extremely unlikely or where the outcome is irrelevant to program goals should be eliminated from the list. The checklist should be directed towards those that will have a meaningful impact on the program, such as impacts on milestones on the critical path. All meaningful risks should be listed in the Top-Level Risk Matrix, Table 1.

Table 2. Risk Categories by Risk Facet

Technica	Opera-bility	Produci-bility	Support-ability	Cost Estimate	Benefit Estimate	Schedule	Manage-ment	Funding	Stake-holder	Informa-tion Security	Human Factors	Safety
Techno-logy System Engineer-ing System Design System Test Technical Documen-tation	System Operat-ion Systems Inter-operabili-ty	Design Produc-tion Manufac-turing Parts & Materials Testing and Docu-menation	Opera-tions & Mainte-nance Logistics Testing & Support Support Documen-tation System Imple-mentation	Manufac-turing Parts & Materials Testing and Docu-menta-tion	Benefit Identifi-cation Benefit Estima-tion	Schedule Estimation Schedule Depen-dency Schedule Manage-ment	Planning Organi-zing Imple-menting Control	Funding Constraint Funding Support Fiscal Manage-ment	Congres-sional Based Adminis-tration Based Aviation Com-munity	Vulner-ability Threat Counter-measures	Usability Suitability Accept-ability	Hazards System failure Mitiga-tion strate-gies

Table 3. Risk Checklist by Risk Facet

Technical Risks	Operability Risks	Producibility Risks
Technology • Undue reliance on currently unavailable or unproved technology • Possible better new technology may be available by time alternative is implemented **System Engineering** • Technically incompatible with NAS Architecture • Inadequate functional analysis • Deficient functional allocation • Incomplete integration • Undefined internal interfaces • Vague operational environment • Insufficient requirements analysis • Unstable requirements • Immature requirements • Weak failure modes analysis • Requirements difficult to trace • Unidentified safety/security considerations **System Design** • Inadequate capacity • Highly complex • Lack of design details • Insufficient design margins • Immature design • Unsatisfactory growth potential • Undefined physical properties • Incomplete hardware design • Incomplete software design • Inadequate software tools • Difficulty of developing real-time, safety critical software • Immature software language • Ineffective fault detection • Inordinate use of unique resources • Complex/incomplete man/machine design • Undefined technical approach **System Test** • Inaccurate/simplistic modeling • Insufficient simulation • No or minimal prototype testing • Incomplete/inadequate test planning • Unsatisfactory OT&E results **Technical Documentation** • Inadequate design documentation • Insufficient test documentation • Ambiguous/incomplete requirements documentation • Undocumented technical details	**System Operation** • Undefined external interfaces • Marginal availability • Insufficient reliability • Inadequate performance • Unsatisfactory OT&E results **Systems Inter-operability** • Operationally incompatible with NAS Architecture • Incompatibilities with Concept of Operations • Incompatibilities with future NAS systems • Places undue loads on other systems • Incompatible or inconsistent operation with existing systems or regulations • Unspecified operational interfaces • Marginal inter-operability	**Design Production** • Highly complex design • Undeveloped production requirements • Inadequate built-in test equipment • Non-standard remote maintenance monitoring • Novel/unproved technologies **Manufacturing** • Deficient manufacturing plan • Novel/unproved manufacturing technologies • Speculative manufacturing strategy • Custom design & manufacture required • Significant special tooling • Undefined tooling requirements • Unclear production requirements • Premature initiation of manufacturing • Unavailable or limited manufacturing facilities • Inadequate quality assurance program • Excessive standards • Unavailable equipment • Inexperienced contractor • Inadequate configuration management process • Insufficient skilled labor • Shallow industrial base **Parts & Materials** • Undefined long lead items • Unavailable gov't furnished equipment • Ineffective incoming materials handling • Unidentified hazardous materials • Unavailable parts **Testing and Documentation** • Inadequate consideration of special test equipment • Insufficient qualification testing • Deficient technical data package • Ineffective factory acceptance test program • Untested design changes

Table 3. Risk Checklist by Risk Facet, continued

Supportability Risks	Cost Estimate Risks	Benefit Estimate Risks	Schedule Risks
O&M • Inadequate O&M concept • Undeveloped O&M strategy • Specialized O&M equipment • Insufficient maintainability • Unsatisfactory maintenance interfaces • Inadequate maintenance procedures • Undeveloped maintenance plan • Configuration management not enforced • Deficient change process **Logistics** • Insufficient spares planning • Spares unavailability • Inaccessible site location • Inadequate training • Unclear Logistics Center responsibilities **Testing & Support** • Insufficient support equipment • Undeveloped support requirements • Inadequate automated test equipment (ATE) • Unidentified field support requirements • Poor diagnostics • Insufficient testing and support facilities • Unskilled/insufficient manpower **Support Documentation** • Deficient technical data • Faulty maintenance plan • Undefined data rights • Inappropriate release cycle **System Implementation** • Deficient implementation approach • Uncertain transition strategy • Unclear rules and procedures • Insufficient personnel/staffing • Unspecified/inappropriate standards	**Cost Estimation** • Inadequate cost estimating tools • Estimation errors • Inaccurate discount rate • Faulty basis of estimates** • Insufficient cost margin • Unrealistic overhead and G&A rates • Relies on scarce resources • Speculative life-cycle costs **Cost Management** • Unsatisfactory cost controls • Insufficient cost monitoring **Product Cost** • Undefined gov't furnished equipment • Unavailable NDI/COTS • Unavailable government facilities • Unavailable contractor facilities • Inadequate budget for tests • Undefined hardware costs • Hidden software costs • Unidentified parts and materials	**Benefit Identification** • Same benefits claimed by other programs • Unidentified major benefits • Unrealistic identified benefits • Difficult to identify benefits **Benefit Estimation** • Benefits not quantifiable • Difficult to estimate benefits • Tenuous relationship to projected benefits • External forces may affect achieving benefits • Erroneous benefits estimations • Inaccurate inflation/discount rates • Speculative cost avoidance • Faulty basis of estimates Inadequate estimating tools	**Schedule Estimation** • Inadequate schedule estimating tools • Erroneous estimations • Faulty basis of estimates • Insufficient schedule margin • Optimistic schedule duration • Inappropriate program schedule **Schedule Dependency** • Unpredictable labor strikes • Improper test scheduling • Excessive task concurrency • Unidentified need for procedures development • Unidentified need for regulations development • Inordinate number of critical path items • Unidentified need for standards development • Uncertainties in contractor process • Uncertainties in contractor stability • Schedule sensitive to technical complexity • Unavailable materials • Unavailable parts • Unavailable government furnished information • Unavailable facilities • Unavailable personnel • Unavailable tools • Unavailable contractor **Schedule Management** • Unsatisfactory schedule controls • Insufficient program schedule monitoring • Improper contractor/subcontractor schedule monitoring

Table 3. Risk Checklist by Risk Facet, continued

Management Risks	Funding Risks	Stakeholder Risks
Planning • Inadequate program plans • Incomplete contingency plans • Deficient risk management plans • Inadequate management approach • Unplanned slips in other programs • Adverse environmental impacts • Unsubstantiated funding profile • Unsubstantiated manpower requirements • Unidentified personnel skills • Minimal resource alternatives • Excessive dependencies on other system • Unexpected acquisition regulation changes **Organizing** • Excessive span of control • Inadequate authority • Undefined responsibilities • Unclear communications • Undefined integration responsibilities • Ambiguous organizational interfaces • Inadequate contractor organization **Implementing** • Insufficient management tools • Inadequate program office staffing • Inadequate resource allocation • Deficient personnel management • Lack of coordination • Tenuous top management support • Cumbersome FAA contracting process • Instability of contractor • Uncertainties in procurement • Unavailable personnel • Deficient change implementation **Control** • Undefined or ineffective change management • Unsatisfactory configuration management • Insufficient contract evaluation • Inadequate planning for contractor monitoring • Insufficient financial management • Irregular/unscheduled program reviews • Insufficient history/records • Undefined key metrics • Uncontrolled requirements changes • Requirements freeze not enforced • Inadequate tracking systems	**Funding Constraint** • Unfavorable agency priorities • Inadequate funding • Unavailable funding • Lengthy budget cycle • Inadequate OMB marks **Funding Support** • Inadequate user support • Ambiguous operator support • Unclear political support • Marginal cost/benefits • Inconsistent FAA plans **Fiscal Management** • Insufficient funding requirements • Insufficient fiscal controls • Insufficient fiscal tools • Insufficient funding plans • Unrealistic funding profile	**Congressional Based** • Impact of congressional mandates • Unfavorable congressional hearings on program • Critical GAO report **Administration Based** • Conflicting FAA priorities • Conflicting DOT priorities **Aviation Community** • Many different stakeholders • Diverse user community • Conflicting user demands • Conflicting user opinions • Conflicting user priorities • Inordinate pressure from user groups • Marginal user support • Strained relationships with users • Resistance to avionics equipage requirements • Inordinate media attention

Table 3. Risk Checklist by Risk Facet, continued

Information Security	Human Factors	Safety
Vulnerability • Incomplete vulnerability assessment • Security policy and procedures not in place • Easy access to communication • No provision for firewalls between shared networks or Virtual Private Networks **Threat** • Incomplete threat assessment on intent and capability to exploit vulnerability • No prioritization of threat severity • No provision for penetration testing • Threat difficulty not considered **Countermeasures** • Few countermeasures defined • Effectiveness of countermeasures on infrastructure not testing • Inadequate configuration audit • Lack of monitoring and enforcement • Insufficient funding tools/controls • Ambiguous funding support	**Usability** • Interface design does not conform to good human engineering design criteria • Workstation layout impairs integration of tasks • Displayed data difficult to read, find or interpret **Functional Suitability** • Automation does not provide the necessary functionality to support effective decision-making/problem-solving • Automation induces new/additional human errors **User Acceptability** • New tasks impose excessive attentional, memory, and workload demands • Requires new teaming and communication links	**Hazards** • Hazards and service-level effects not fully identified • Inter-relationship of hazard effects not established • Hazards not classified per common scheme • Hazard class not based on operational environment definition **System Safety Interdependence** • Hazard interdependence poorly understood • Interoperability of components on system safety not investigated • Systemic approach to safety is lacking one or more components (planning, requirements, procedures, operation, aircraft certification, user approval) **Mitigation Strategies** • Mitigation strategies not shared • Operational and safety objective not established • Lack of critical/valid safety information • Mitigation strategies not tied to hazards or safety requirements • Plan for development and operational assurance not in place

4.2 Step 2 - Estimate Probability of an Adverse Event

Once the risks are identified for each alternative using Tables 1, 2, and 3, a risk score (i.e., Overall Weighted Alternative Risk Score) is determined for each risk facet, and then an overall risk rating (i.e., Overall Alternative Risk Rating) is generated for each alternative. In spite of attempts to be analytic about quantifying risks, considerable subjectivity remains. The degree of risk perceived in a given situation is partially a reflection of the personality of the risk assessor(s). A risk-rating scheme built against a set of definitions provides a framework for eliminating some of the ambiguity. Further, the rating scheme should be simple. The following risk rating scheme involves determining a High, Medium, or Low overall risk rating using the notion that the degree of risk is a judgement reflecting the probability of occurrence of an adverse event and the severity of impact on the alternative should the adverse event occur.

If a particular risk facet does not apply to the alternatives being assessed, then the probability of an adverse event and the severity of the impact of the adverse event do not need to be estimated for that risk facet.

For each risk facet, the probability of occurrence of an adverse event (expressed as High, Medium, or Low) is determined using Table 4, Estimating the Probability of an Adverse Event, as guidance. The result is entered in the second column of Table 6, Determining Risk Score.

Four possible methods to estimate the probability of occurrence and severity of impact are briefly described below. More than one method, as well as approaches other than those listed below, can be used.

- Expert Interviews - This process involves identifying expert(s) and methodically questioning them about the risks in their area of expertise as related to the alternative. Data collection sheets can be used to facilitate this process. The questioning focuses on extracting information about what the program risks are and their relative magnitude.

- Analogy Comparisons - The analogy comparisons and lessons learned techniques for risk identification and quantification are based on the idea that no new program, no matter how advanced or unique, represents a totally new concept or system. The process involves assessing risk by using data from similar prior programs.

- Evaluation of Program Plans - This technique highlights and isolates risks caused by insufficiencies and disparities in planning. It evaluates program plans for contradictions and voids. The plans do not need to be formal plans, but could include program management plans, acquisition plans, specifications, statements of work, or work breakdown structures. The process assesses the plans for correctness, completeness, currency, and consistency.

- Delphi Technique - The Delphi technique is a method to structure intuitive thinking by a group and produce technological forecasts. It can be used for the systematic collection and collation of informed judgments obtained from a group of experts and for the refinement of these judgments by an integrative process to arrive at a joint judgment or decision. Typically, judgments of the individuals in a group are collected, perhaps integrated as a group response, and fed back to the individuals. Each individual then considers whether to contribute more information or to modify earlier views. This iterative process is continued until a reasonable consensus is obtained. The responses can be fed back anonymously if desired.

4.3 Step 3 - Estimate Severity of Impact of an Adverse Event

For each risk facet, the severity of the impact of the adverse event on the alternative (expressed as Substantial, Moderate, or Minor) is determined using Table 5, Estimating the Severity of Impact of an Adverse Event, as guidance. The result is entered in the third column of Table 6.

The four possible methods described in Section 4.2 to estimate the probability of occurrence of an adverse event can be used to estimate the severity of impact. Again, more than one method, as well as approaches other than those listed, can be used.

Table 4. Estimating the Probability of an Adverse Event Impacting the Program

Facet	High Probability of an Adverse Event	Medium Probability of an Adverse Event	Low Probability of an Adverse Event
Technical	Design unknown. Approach to meet requirements carried only through conceptual design and analysis. Technology is only concept or experimental.	Design is in development or prototype phases. Technology prototype or engineering model tested in relevant environment but not operated in fielded environment.	Design is mature. Technology within state-of-the-art or off the shelf. Performance specifications are known.
Operability	NAS or other interfaces not fully known or documented. Operational concept or implementation of concept has yet to be established. Significant impacts are likely to procedures, which would cause operational implementation to be unsuccessful.	NAS or other interfaces somewhat known and partially documented. Operational concept has evolved to the point of a design baseline. Impacts are likely to several procedures, which may cause operational implementation to be unsuccessful.	NAS or other interfaces are known and documented. Design approaches for the operational concept have been demonstrated or implemented. Will impact a few procedures but operational implementation is expected to be successful.
Producibility	Manufacturing and production capabilities not known or unavailable.	Manufacturing or production capabilities in state of change.	Manufacturing and production capabilities known and available.
Supportability	New support technologies and procedures or substantial modifications to existing support technologies or procedures will be required which could prevent suitable transition of support to AF.	Items similar in concept have been supported as fielded systems or supported during test. Substantial modifications may be required to existing support technologies or procedures and transition of support to AF may be difficult.	Similar items have been fielded & are currently being supported, or similar items have been demonstrated to be supportable during field testing. Only minor changes to existing support technologies or procedures will be required. Transition of support to AF will be straightforward.

Table 4. Estimating the Probability of an Adverse Event Impacting the Program, continued

Facet	High Probability of an Adverse Event	Medium Probability of an Adverse Event	Low Probability of an Adverse Event
Cost Estimate	Basis for cost estimation is inadequate, or major uncertainties exist related to the scope/definition required for estimation.	Cost factors not certain, but scope/definition required for estimation is adequate.	Cost factors understood and based on or extrapolated from similar items in production. Definition required for estimation is adequate.
Benefit Estimate	Major uncertainties exist related to benefit estimation; extremely tenuous relationship of alternative to projected benefits; or very likely external forces will affect achieving benefits.	Benefits not certain, but scope/definition required for estimation is adequate; slightly tenuous relationship of alternative to projected benefits; or possible external forces may have some affect on achieving benefits.	Benefits understood and based on or extrapolated from similar items in operation. Definition required for estimation is adequate. Direct relationship of alternative to benefits. Little likelihood of external forces affecting the achievement of the benefits.
Schedule	Many schedule interdependencies for which there is little or no flexibility to absorb delays. Few or no plans to minimize unknowns; difficult or complex system to develop. Knowledge and experience base very limited.	Some schedule interdependencies with little schedule margin. Plans to minimize unknowns are generally complete; some uncertainties exist. Little knowledge and experience in some areas.	Adequate schedule with substantial margins and achievable plans to minimize unknowns. High knowledge and experience base. There are no schedule dependencies beyond the control of the alternative.
Information Security	Vulnerability and threat assessments not planned or conducted. Countermeasures not identified or tested.	Vulnerability and threat assessment planned but not conducted. Theoretical countermeasures identified	Vulnerability and threat assessments conducted. Countermeasures developed for each threat, and their ability to withstand threats proved.

Table 4. Estimating the Probability of an Adverse Event Impacting the Program, continued

Facet	High Probability of an Adverse Event	Medium Probability of an Adverse Event	Low Probability of an Adverse Event
Human Factors	Perceptual and physical characteristic of the interface does not support standard tasks. Information and automated functions for supporting decision-making are inadequate. User tasks and skills not well defined and do not conform to current skill levels.	Empirical human-in-the-loop testing has been conducted in a lab environment but not in the field. User requirements to detect and mitigate system error have been partially identified. User tasks and skills defined but user changing roles require reevaluation of skills and training.	Interface design is mature and compatible with user expectation of how the system works. Testing has been completed. Automation provides full functionality to support user decision-making. User tasks and skills are well defined or remain essentially unchanged.
Safety	Hazards and their impact on NAS services inadequately defined. Interdependency of system components in contributing to system failure poorly considered. Mitigation strategies not directly tied to hazards. Mitigation measures border on being unpalatable.	Process for assessing safety developed and applied. Mitigation measured are identified and related to hazards. Mitigation strategies are palatable.	Mitigation strategies are funded and applied.
Management, Funding and Stakeholder	Management, funding and stakeholder facets and environments not known or unstable.	Management, funding and stakeholder facets and environments in state of change but somewhat known.	Management, funding and stakeholder facets and environments known and stable.

Table 5. Estimating the Severity of an Adverse Event Impacting the Program

Facet	Substantial Severity of Impact	Moderate Severity of Impact	Minor Severity of Impact
Technical	Performance or problem data indicate that with current alternative design margins, full performance would not be met and alternate systems are not available.	Performance or problem data indicate that with current alternative design margins full performance objectives will only be met by: (1) significant modification to a design of a component or subsystem; or (2) reallocation of design margins among subsystems.	Performance and problem data indicate that only minor hardware/software design changes will be needed to meet full performance objectives.
Operability	No operationally suitable solutions available without major impacts on the overall system performance. Will cause significant impact to existing procedures, which could cause operational implementation to be unsuccessful.	Technical operationally suitable solutions partially identified. The solution is not readily available or will have significant impacts on the overall system performance. Will impact several procedures and may cause operational implementation to be only partially successful.	Technical operationally suitable solution is identified and readily available. Will impact a few procedures but operational implementation is expected to be successful.
Producibility	Manufacturing and production capabilities not known or unavailable.	Manufacturing or production capabilities in state of change, and some uncertainty exists about when capabilities will be available.	Manufacturing and production capabilities known and available.
Supportability	System design characteristics & planned logistics and software support resources do not meet system utilization requirements. Support procedures or technologies will be significantly impacted and could prevent suitable transition of support to AF.	System design characteristics & planned logistics and software support resources meet some but not all system utilization requirements. Some support procedures or technologies will be impacted and transition of support to AF may be difficult.	System design characteristics & planned logistics and software support resources meet nearly all system utilization requirements. Only minor support procedures or technologies will be impacted, and transition of support to AF highly likely to be successful.
Benefit Estimate	Less than 75% of the estimated benefits are expected to be achieved.	75 - 90% of the estimated benefits are expected to be achieved.	At least 90% of estimated benefits are expected to be achieved.

Table 5. Estimating the Severity of an Adverse Event Impacting the Program, continued

Facet	Substantial Severity of Impact	Moderate Severity of Impact	Minor Severity of Impact
Cost Estimate	Estimated costs are likely to be exceeded by more than 25 %	Estimated costs are likely to be exceeded by 10 - 25 %	Estimated costs are likely to be exceeded by less than 10 %
Schedule	A schedule slip of more than 25% is expected.	A schedule slip of 10% — 25% is expected.	A schedule slip of less than 10% is expected.
Information Security	Information security protection at the system perimeter and at the workstations and servers are not provided. Information security infrastructure and intrusion detection hardware and software is not available or not acceptable.	Some information security infrastructure is available for some NAS systems/subsystems including dial-up protection for remote users. Some intrusion detection hardware and software are available.	Complete information security infrastructure is available for every NAS system/subsystem including intrusion detection hardware and software.
Human Factors	Computer-human interface and automated functions for supporting standard interaction tasks and decision-making/problem solving activities are inadequate. High probability of human error, increased workload, and probable system performance low. Potential job satisfaction in the context of technology upgrades is low.	Prototype testing of the interface occurs in relevant environment but not in field environment. Potential weakness of the interface identified but not mitigated. Automation provides partial functionality to support decision-making/problem solving activities. Potential job satisfaction in the context of technology upgrades is undetermined.	Computer-human interface is mature and automation provides full functionality to support decision-making/problem solving activities. Opportunities for job satisfaction are supported or enhanced by technology upgrades.
Safety	Safety level objective/requirements /hazards not identified for future NAS systems nor is acceptability criteria known.	Safety level objectives/requirements are identified but hazards for future NAS systems remain uncertain.	Safety level objectives/requirements/ hazards are identified, as well as the acceptability criteria for each safety level objective and requirement.
Management, Funding and Stakeholder	Management, funding and stakeholder facets and environments not known and will adversely impact the alternative.	Management, funding and stakeholder facets and environments in state of change but somewhat known, and may incrementally impact the alternative.	Management, funding and stakeholder facets and environments known and stable, and may only insignificantly impact the technical alternative.

Table 6. Determining Risk Score

Facet	Probability of an Adverse Event (High, Medium, Low)	Severity of Impact (Substantial, Moderate, Minor)	Facet Risk Rating (0-10) (from Table 7)	Facet Weight (0-1)	Weighted Facet Score (0-10)
Technical					
Operability					
Producibility					
Supportability					
Cost Estimate					
Benefit Estimate					
Schedule					
Management					
Funding					
Infosec					
Human Factors					
Safety					
Stakeholder					
Overall Weighted Alternative Risk Score					

4.4 Step 4 - Assign Risk Facet Ratings

Assign a Facet Risk Rating Score using the assignment scheme shown in Table 7, Risk Facet Rating Score Assignments, and enter the facet score in the fourth column of Table 6. This assignment is done for all risk facets relevant to the alternative.

Table 7. Risk Facet Rating Score Assignments

	Severity of Impact		
Probability of an Adverse Event	**Substantial**	**Moderate**	**Minor**
High	10	8	5
Medium	8	5	2
Low	5	2	0

4.5 Step 5 - Calculate Overall Alternative Risk Rating

The final step in assessing the risk for any alternative is to calculate an overall risk rating for the alternative by rank-ordering all the risk facets based on the perceived risk each one represents to the overall program. A numerical weight is then assigned to each risk facet reflecting its importance relative to other facets within the rankings (i.e., a facet's importance compared to the importance of the facets directly preceding and following it in the rankings). (Note: A predetermined cumulative total should be used.) The weights should then be "normalized" so that the cumulative total equals 1.00 (i.e., the weights should be between zero and 1.00 with the cumulative total equaling 1.00). (Note: A weight of zero means that the risk facet does not apply (i.e., it falls below the threshold of what is important compared to the other facets) and a weight of 1.00 means that only that risk facet applies (i.e., it far exceeds the threshold of what is important compared to the other facets).) The ranking and assignment of weights should be the same for all alternatives and based on a team (e.g., ASD and the sponsoring program office) consensus before the risk assessment process is conducted. Once agreed upon, the weights must remain the same for all alternatives.

The weights are then entered into the fifth column of Table 6. And finally, the Weighted Facet Score for each risk facet is calculated by multiplying the entries in the fourth and fifth columns and entering the results into the last column of Table 6. The overall weighted average alternative risk score is entered in the bottom row of Table 6 by adding the individual weighted risk facet scores in the last column.

Once the Overall Weighted Alternative Risk Score is calculated for each alternative (refer to Table 6), a descriptive alternative risk rating (i.e., High, Medium, or Low) is calculated using Table 8. This rating can also be entered into a common table to permit comparison of risk assessment results across alternatives (refer to Table 9).

Table 8. Overall Alternative Risk Rating

Overall Rating (Score)	Description
High (7.0— 10)	Alternatives with High Overall Risk Rating should receive close attention. Risk facets with High Risk Ratings should be considered Principal Risks. Each High Risk should have strategies, metrics, and a plan of action and milestones developed by the risk owner and be aggressively managed. They should be monitored and managed on a continuous basis until the risk is mitigated to an acceptable level.
Medium (3.0 — 6.99)	Alternatives with a Medium Overall Risk Rating require attention. Risk facets should be examined to see if any are rated high and should be placed on the Principal Risk List and managed as described above. Each Medium Risk should have candidate strategies, metrics and a plan of action and milestones developed by the risk owner and should be managed and reviewed frequently. Any risks on the Principal Risk List should be aggressively monitored and managed on a

	continuous basis until the risk is mitigated to an acceptable level.
Low (0 — 2.99)	Alternatives with a Low Overall Risk Rating do not normally require attention for risk. However, status should be reviewed periodically by the risk owner. Any high or medium risk facets should receive attention as described above.

It may be desired to determine a risk rating for a subset of risk facets, such as the risk of the alternative output performing as designed which might involve combining the risk facets of Technical, Operability, and Supportability. A risk rating for a subset of risk facets can be determined by summing the weighted facet scores (last column of Table 6) for risk facets in the subset. In the above example, the weighted facet scores for Technical, Operability, and Supportability would be summed to give a score for the risk of the alternative output performing as designed.

4.6 Step 6 - Compare Risks among Alternatives

The risk assessment process is repeated to determine an overall risk rating for each alternative. The individual risk facet ratings and the overall risk rating for all alternatives can be entered into a table, such as Table 9, Risk Ratings of Alternatives, to permit comparison of risk assessment results across alternatives.

Table 9. Risk Ratings of Alternatives

Risk Assessment Ratings	Alternative 1	Alternative 2	Alternative 3	Alternative . . .
Technical				
Operability				
Producibility				
Supportability				
Cost Estimate				
Benefit Estimate				
Schedule				
Management				
Funding				
Infosec				
Human Factors				
Safety				
Stakeholder				
Overall Weighted Alternative Risk Score				
Overall Alternative Risk Rating (H, M, L)				

To facilitate cross comparison of alternatives, Table 9 cells may be filled with colorful green, yellow, and red shading to represent the alternatives' relative risk rating. Any risk facet receiving a score of 10, using Table 7 shall be shaded red for high risk. The same high risk designation is reasonable for any risk facet receiving a score of 8. This is consistent with Table 8 score ratings. Similarly, any facet receiving a score of 5, shall be shaded yellow or white to represent medium risk. Lastly any facet receiving a score of 2 or 0, shall be shaded green for low risk. In this way, the individual risk of each facet can instantly be identified and compared.

The risk assessment results contained in Table 9 should be used with the other evaluation factors (i.e., life cycle costs, benefits, schedule, and performance) to narrow the set of alternatives to the most promising one(s) for presentation to the Joint Resources Council (JRC) and to justify those in the subset. The JRC can also use Table 9 as part of their decision information.

Intentionally Left Blank

5.0 USE OF OUTPUTS OF THE RISK ASSESSMENT PROCESS THROUGHOUT ACQUISITION PROCESS

Once the risk assessment process has been completed and the preferred alternative is selected by the JRC, the Top-Level Risk Matrix, Table 1, and its supporting risk documentation should be handed off to the responsible program office. The Top-Level Risk Matrix should be continually used and updated for managing program risk throughout the acquisition process.

Furthermore, a Risk Watchlist should be prepared from the Top-Level Risk Matrix to serve as a worksheet for managers in managing risk throughout the program life cycle. For example, there may be scheduling risks in the test phase due to other projects using the test facilities. Another possible risk is that new technology may become available in the middle of the development phase and a decision would have to be made to proceed with the original development or delay the program until the new technology is ready for development. The Risk Watchlist provides a convenient form to track the status of such potential risks and to document actions in managing risk.